# Protecting Personal Data When Working Remotely

**Measures to control and prevent the spread of COVID-19 will involve more people working remotely than usual. Below are some tips to keep personal data safe when working away from the office. For more information you can consult the guidance on data security on our website.**

## Devices

- Take extra care that devices, such as USBs, phones, laptops, or tablets, are not lost or misplaced.
- Make sure that any device has the necessary updates, such as operating system updates (like iOS or android) and software/antivirus updates.
- Ensure your computer, laptop, or device, is used in a safe location, for example where you can keep sight of it and minimise who else can view the screen, particularly if working with sensitive personal data.
- Lock your device if you do have to leave it unattended for any reason.
- Make sure your devices are turned off, locked, or stored carefully when not in use.
- Use effective access controls (such as multi-factor authentication and strong passwords) and, where available, encryption to restrict access to the device, and to reduce the risk if a device is stolen or misplaced.
- When a device is lost or stolen, you should take steps immediately to ensure a remote memory wipe, where possible.

## Emails

- Follow any applicable policies in your organisation around the use of email.
- Use work email accounts rather than personal ones for work-related emails involving personal data. If you have to use personal email make sure contents and attachments are encrypted and avoid using personal or confidential data in subject lines.
- Before sending an email, ensure you're sending it to the correct recipient, particularly for emails involving large amounts of personal data or sensitive personal data.

## Cloud and Network Access

- Where possible only use your organisation's trusted networks or cloud services, and complying with any organisational rules and procedures about cloud or network access, login and, data sharing.
- If you are working without cloud or network access, ensure any locally stored data is adequately backed up in a secure manner.

## Paper Records

- It's important to remember that data protection applies to not only electronically stored or processed data, but also personal data in manual form (such as paper records) where it is, or is intended to be, part of filing system.
- Where you are working remotely with paper records, take steps to ensure the security and confidentiality of these records, such as by keeping them locked in a filing cabinet or drawer when not in use, disposing of them securely (e.g. shredding) when no longer needed, and making sure they are not left somewhere where they could be misplaced or stolen.
- If you're dealing with records that contain special categories of personal data (e.g. health data) you should take extra care to ensure their security and confidentiality, and only remove such records from a secure location where it is strictly necessary carry out your work.
- Where possible, you should keep a written record of which records and files have been taken home, in order to maintain good data access and governance practices.

An Coimisiún um Chosaint Sonraí
Data Protection Commission